

REMARKS

In this Amendment, Applicant has amended Claim 1 to rephrase certain expression. The amendment is editorial in nature. It is respectfully submitted that no new matter has been introduced by the amended. All claims are now present for examination and favorable reconsideration is respectfully requested in view of the preceding amendments and the following comments.

OATH/DECLARATION:

It is respectfully submitted that the Substitute Declaration was submitted on May 10, 2004. The copies of the transmittal letter, the postcard with date stamp and the Substitute Declaration are enclosed herewith for Examiner's reference. Therefore, withdrawal of the objection to the declaration is respectfully requested.

CLAIM OBJECTION:

Claim 1 has been objected because of containing certain informality. It is respectfully submitted that the objection has been overcome by the replacing the word "alternate" with the phrase "by turn." Therefore, withdrawal of the objection to the declaration is respectfully requested.

REJECTIONS UNDER 35 U.S.C. § 102:

Claims 1 – 2 have been rejected under 35 U.S.C. § 102 (b) as allegedly being anticipated by Delayaye et al (US 4,751,733), hereinafter Delayaye.

Applicant traverses the rejection and respectfully submits that the present-claimed invention is not anticipated by the cited reference, because Delayaye does not disclose or teach all the elements of the embodiments of the present invention as claimed.

More specifically, in the embodiments of the present invention as claimed, “an operation of transposing bits of i -th subblock is used as the operation dependent on the value of j -th subblock” (Claim 1). Therefore, operations on data subblocks are performed depending on data being converted, according to the embodiments of the present invention. However, in Delayaye, data subblocks are performed depending on the key or under the control of the key. It is respectfully submitted that this feature is repeatedly emphasized in the specification in Delayaye, such as the descriptions at col. 1, lines 13 – 14 and lines 54 – 62; col. 2, lines 60 – 65; col. 8, lines 51 – 55; and col. 9, lines 3 – 7.

For example, at col. 9, lines 3 – 7, Delayaye clearly indicates that, for the given fixed key, the memory of the claimed device stores one substitution table to perform the encryption algorithm and one more substitution table, according to which the substitution reverse to the first one is performed, to perform the decryption algorithm. The structure of the substitution tables is described at col. 6, lines 29 – 38. It corresponds to the typically used tables for performing substitution operations on data subblocks in encrypting to ensure the possibility of performing the reverse substitution, which is necessary to enable deciphering the converted data back. According to the above tables, it is in principle impossible to perform substitution depending on the data being converted as in the embodiments of the present invention. This means that, in Delayaye, substitution operation is performed on data subblocks that depends solely on the keys, but not on the input data block or some other data subblock. If the method of Delayaye includes performing substitution operations on some subblocks depending on other ones, conversion would become irreversible and it would not be possible to expressly restore the plain text based in the cipher text. Therefore, Delayaye fundamentally cannot perform reversible conversion when data subblocks of their parts are placed in blocks 21 and 20 in Fig. 3 (LATCH blocks).

Applicant respectfully submits that the Examiner has misinterpreted or broadened the disclosure of Delayaye, especially, descriptions at col. 8, lines 45 – 50, which teaches

how key-dependent substitution operation is implemented. Indeed, performing on i-th data subblock fixed substitution operation consists in addressing the memory according to the value of the i-th data subblock, and performing on the i-th data subblock controlled key-dependent substitution operation consists in addressing the memory according to the value of the i-th data subblock and the value of the subkey. By fixing the key, some substitution table is fixed. For example, in fixing the key, addressing the memory is effected only within the table setting the fixed substitution on the data subblock (see description of the substitution table structure in lines 29 – 38, col. 6).

Applicant respectively submits that the embodiments of the present invention as claimed include different features from the disclosure of Delayaye. Delayaye does not disclose the feature of performing on data subblocks controlled transpositions dependent on the data being converted. The encryption method implemented by the device of Delayaye discloses performing in data subblocks key-dependent controlled substitutions.

Therefore, the presented claims are not anticipated by Delayaye and the rejection under 35 U.S.C. § 102 (b) has been overcome. Accordingly, withdrawal of the rejections under 35 U.S.C. § 102 (b) is respectfully requested.

REJECTIONS UNDER 35 U.S.C. § 103:

Claim 3 has been rejected under 35 U.S.C. § 103, as allegedly being obvious and unpatentable over Delayaye, in view of Mittenthal, Statically Efficient Inter-Road Mixing Block Substitute Devices, January 1996, hereinafter Mittenthal.

Applicant traverses the rejection. It is respectfully submitted that the cited references fail to render the embodiments of the present invention as claim obvious. As stated above, Delayaye failed to teach the feature that “an operation of transposing bits of i-th subblock is used as the operation dependent on the value of j-th subblock”. By its dependency on Claim 1, Claim 3 also includes this feature. Therefore, even if Delayaye and Mittenthal are combined, they will not achieve the present invention as claimed.

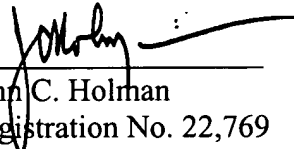
Nowhere in prior art has suggestion or incentive to combine Delayaye and Mittenthal to achieve the invention as presently claimed. Even if they are combined, they do not disclose or teach the invention as presently claimed. One of ordinary skilled in the art would not discern the present invention at the time of its invention. Therefore, the rejection under 35 U.S.C. § 103 has been overcome. Accordingly, withdrawal of the rejection under 35 U.S.C. § 103 is respectfully requested.

Having overcome all out standing grounds of rejection, the application is now in condition for allowance, and prompt action toward that end is respectfully solicited.

Respectfully submitted,

JACOBSON HOLMAN PLLC

Date: October 29, 2004
(202) 638-6666
400 Seventh Street, N.W.
Washington, D.C. 20004
Atty. Dkt. No.: P65724US0

By 
John C. Holman
Registration No. 22,769

Enclosures:

Copies of previously filed Substitute Declaration and transmittal letter.